

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

**Defective images within this document are accurate representation of
The original documents submitted by the applicant.**

Defects in the images may include (but are not limited to):

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000269950 A**

(43) Date of publication of application: **29 . 09 . 00**

(51) Int. Cl.

H04L 9/08
G09C 1/00

(21) Application number: **11066405**

(22) Date of filing: **12 . 03 . 99**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **HARADA TOSHIHARU**
TATEBAYASHI MAKOTO

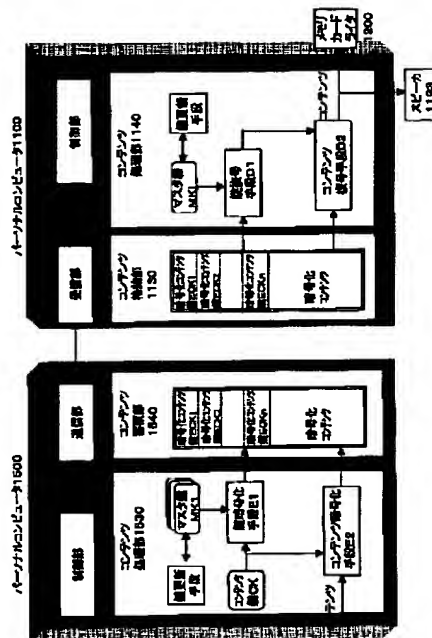
(54) **COPYRIGHT PROTECTION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To save labor and time required for ciphering data by ciphering contents key into a ciphered contents key, ciphering contents into ciphered contents, decoding the ciphered contents key by using a master key, and updating or invalidating the master key.

SOLUTION: A contents processing part 1530, once receiving a generation indications for contents and information of the contents from a control part, generates a contents key CK and performs a ciphering process by using a key ciphering means E1 by using the contents key CK. Furthermore, the contents are ciphered by a contents ciphering means by using the contents key CK. Capsule data, as data including the ciphered contents and contents keys FEK1 to ECKn, are outputted to a contents storage part 1540. A content update device once receiving a contents update indication, the capsule data, and the master key to be invalidated invalidates the ciphered contents keys of the capsule data.

COPYRIGHT: (C)2000,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-269950
(P2000-269950A)

(43) 公開日 平成12年9月29日 (2000.9.29)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 9 A 0 0 1
		H 0 4 L 9/00	6 0 1 E

審査請求 未請求 請求項の数4 O L (全 9 頁)

(21) 出願番号 特願平11-66405

(22) 出願日 平成11年3月12日 (1999.3.12)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

Fターム (参考) 5J104 AA01 AA13 AA16 AA34 EA06

EA18 NA02 NA37 PA14

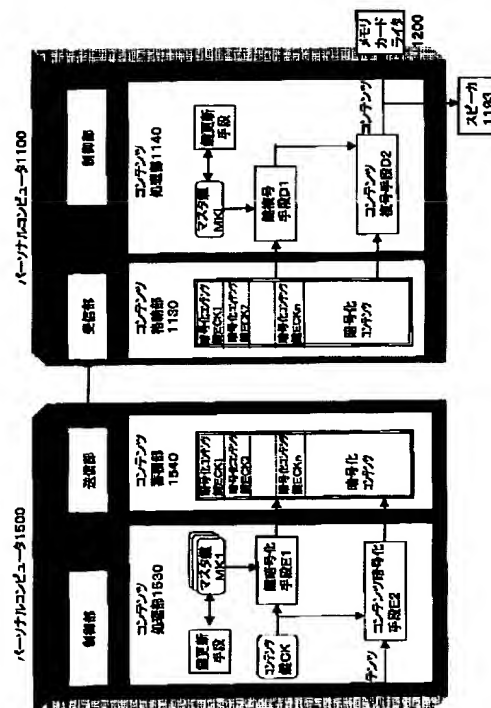
9A001 EE03 JJ13 JJ25 LL03

(54) 【発明の名称】 著作物保護システム

(57) 【要約】

【課題】 著作物データ (コンテンツ) を暗号化して配布するシステムにおいて、暗号化されたコンテンツの複号に用いる鍵の盗難に対処するため、鍵を更新できるシステムを提供する。

【解決手段】 第1の装置は、第1から第nのマスタ鍵を用いてコンテンツ鍵を暗号化し、コンテンツ鍵を用いてコンテンツを暗号化する。第2の装置は、前記第1から第nのマスタ鍵のうちのいずれかである第jのマスタ鍵を用いて、第jの暗号化コンテンツ鍵を復号し、コンテンツ復号鍵を用いて、暗号化コンテンツを復号する。第jのマスタ鍵が盗難した場合、第1の装置及び第2の装置における第jのマスタ鍵を無効にするもしくは第n+1のマスタ鍵に更新する。



【特許請求の範囲】

【請求項 1】 デジタル著作物であるコンテンツの配送システムにおける著作物保護システムであって、第 1 から第 n のマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第 1 から第 n の暗号化コンテンツ鍵を作成する鍵暗号化手段と、

前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、

前記第 1 から第 n のマスタ鍵のうちのいずれかである第 j のマスタ鍵を用いて、前記第 j の暗号化コンテンツ鍵を復号することによりコンテンツ鍵を取得する鍵復号手段と、

前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、

前記鍵暗号化手段および前記鍵復号手段で利用される前記第 j のマスタ鍵を無効にするもしくは前記第 j のマスタ鍵を第 n + 1 のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする著作物保護システム。

【請求項 2】 著作物保護システムはさらに、前記鍵暗号化手段で作成された第 1 から第 n の暗号化コンテンツ鍵のうち前記第 j の暗号化コンテンツ鍵を無効にする、もしくは、前記第 j の暗号化コンテンツ鍵を、コンテンツ鍵を第 n + 1 のマスタ鍵を用いて暗号化した結果である第 n + 1 の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることを特徴とする請求項 1 記載の著作物保護システム。

【請求項 3】 前記鍵暗号化手段もしくは前記鍵復号手段は、それぞれ鍵暗号化用もしくは鍵復号用のソフトウェアを実行するパーソナルコンピュータで構成され、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化用もしくは鍵復号用のソフトウェアが、前記第 n + 1 のマスタ鍵を利用した前記鍵暗号化用もしくは鍵復号用のソフトウェアに置き換えられることを特徴とする請求項 1 記載の著作物保護システム。

【請求項 4】 前記鍵暗号化手段もしくは前記鍵復号手段は、それぞれ鍵暗号化もしくは鍵復号処理を実行するハードウェアで構成され、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化もしくは鍵復号処理が、前記第 n + 1 のマスタ鍵を利用した前記鍵暗号化もしくは鍵復号処理に切り替えられることを特徴とする請求項 1 記載の著作物保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル著作物の著作権保護を技術的に実現するためのシステムに関し、特に、デジタル著作物たるコンテンツの再生記録における著作物保護技術に関する。

【0002】

【従来の技術】 近年、インターネット関連技術の発展により、音楽等のコンテンツをインターネットを通じて配送し、これをダウンロードしたユーザから料金を受け取ることも可能となってきた。

【0003】 またインターネットからパーソナルコンピュータにダウンロードされたデジタル著作物が簡単に複製できるものであるため、これを防止するために、暗号化等の技術が用いられている。

【0004】

【発明が解決しようとする課題】 ところで、このように、各種コンテンツを暗号処理して配布する場合、暗号化を行う装置に暗号鍵を持たせ、復号を行う装置に復号鍵を持たせて暗号処理して配布を行うのが一般的である。なお、ここでは、“暗号鍵による暗号化”という表現で、署名生成鍵による署名生成変換を、“復号鍵による復号”という表現で、署名検証鍵による署名検証変換処理を含む広い意味で用いている。

【0005】 しかしながら、復号鍵が盗難した場合、暗号装置及び復号装置において、盗難した復号鍵および対応する暗号鍵を無効にしたり更新するとともに、各種データに対して新しい暗号鍵で再度暗号化する必要が生じる。再度暗号化する手間は、すでに暗号化したデータの量に比例して大きくなる。

【0006】 本発明は、このような鍵更新に伴う、データの暗号処理の手間を軽減するを提供することを目的とする。

【0007】

【課題を解決するための手段】 上記目的を達成するために、本発明は、第 1 から第 n のマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第 1 から第 n の暗号化コンテンツ鍵を作成する鍵暗号化手段と、前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、前記第 1 から第 n のマスタ鍵のうちのいずれかである第 j のマスタ鍵を用いて、前記第 j の暗号化コンテンツ鍵を復号することによりコンテンツ鍵を取得する鍵復号手段と、前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、前記鍵暗号化手段および前記鍵復号手段で利用される前記第 j のマスタ鍵を無効にするもしくは前記第 j のマスタ鍵を第 n + 1 のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする。

【0008】 また、著作物保護システムはさらに、前記鍵暗号化手段で作成された第 1 から第 n の暗号化コンテンツ鍵のうち前記第 j の暗号化コンテンツ鍵を無効にする、もしくは、前記第 j の暗号化コンテンツ鍵を、コンテンツ鍵を第 n + 1 のマスタ鍵を用いて暗号化した結果である第 n + 1 の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることを特徴とする。

【0009】 また、前記鍵暗号化手段もしくは前記鍵復

号手段は、それぞれ鍵暗号化用もしくは鍵複号用のソフトウェアを実行するパーソナルコンピュータで構成され、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウェアが、前記第 $n+1$ のマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウェアに置き換えられることを特徴とする。

【0010】また、前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化もしくは鍵複号処理を実行するハードウェアで構成され、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理が、前記第 $n+1$ のマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理に切り替えられることを特徴とする。

【0011】

【発明の実施の形態】以下、本発明に係わる著作物保護システムの実施の形態である音楽コンテンツ配信システムについて、図面を用いて説明する。

【0012】＜構成＞図1は、本発明に実施の形態に係る音楽コンテンツ配信システム1000の概観図である。

【0013】音楽コンテンツ配信システム1000は、パーソナルコンピュータ1500により、音楽コンテンツを作成送信し、通信回線1001を介して受信した音楽コンテンツをパーソナルコンピュータ1100により再生し、また、メモリカード1300に記録するシステムである。なお、メモリカード1300は、厚さ数ミリ、縦横2cm四方程度の形状で、64メガバイトの記憶容量を持ち制御回路を内蔵する半導体メモリである。ユーザは、このメモリカード1300を、メモリカード再生機器に挿入することにより、ヘッドフォン等を通じて再生された音楽を楽しむことができる。

【0014】パーソナルコンピュータ1500は、CPU、メモリ、ハードディスク等を内蔵し、コンテンツ提供者の指示に応じて音楽コンテンツ作成用プログラムを実行することができるものであり、通信回線1001と接続されている。

【0015】パーソナルコンピュータ1100は、CPU、メモリ、ハードディスク等を内蔵し、ユーザの指示に応じて音楽コンテンツ再生用プログラムを実行することができるものであり、スピーカ1193、及び、通信回線1001と接続されており、また、いわゆるPCカードスロットであるメモリカードライタ挿入口1195を有する。

【0016】メモリカードライタ1200は、いわゆるPCカードであり、メモリカードを挿入するためのメモリカード挿入口1299を有している。

【0017】図2は、音楽コンテンツ配信システム1000の機能ブロック図である。

【0018】機能的には、まず、コンテンツの提供者が

利用するパーソナルコンピュータ1500（以下提供者側PCと称する）は、送信部1510と、制御部1520と、コンテンツ処理部1530、コンテンツ蓄積部1540とから構成される。ユーザが利用するパーソナルコンピュータ1100（以下ユーザ側PCと称する）は、受信部1110と、制御部1120と、コンテンツ格納部1130と、コンテンツ処理部1140とから構成される。また、スピーカ1193と、メモリカードライタ1200が接続される。

【0019】同図には、コンテンツ処理部により作成された暗号化された状態のコンテンツ（以降、カプセルデータ100と呼ぶことにする）をも示している。カプセルデータは、通信回線からユーザが利用するパーソナルコンピュータに入力されるデータであり、音楽コンテンツとこれに関する管理情報などが暗号化されたものである。カプセルデータの内容については後程詳しく説明する。

【0020】提供者側PC1500における送信部1510と制御部1520と、コンテンツ処理部1530とは、パーソナルコンピュータ1500のメモリに格納された音楽コンテンツ生成用プログラムが、CPUにより実行されることにより実現される機能であり、コンテンツ蓄積部1540は、パーソナルコンピュータ1500のメモリ又はハードディスクの一領域である。

【0021】音楽コンテンツ生成用プログラムは、生成する音楽コンテンツの内容をコンテンツ提供者に選択させたり、選択されたコンテンツに対する課金条件を受け付けるためのものであり、制御部1520は、キーボードによる提供者の操作を受け付け、これに応じて、音楽コンテンツの生成を行うものである。

【0022】コンテンツ処理部1530は、制御部1520からのコンテンツの生成指示と、コンテンツの情報を受け取ると、コンテンツ鍵CKを生成し、このコンテンツ鍵CKを、 n 個のマスタ鍵MK1、…、MK n を用いて、それぞれ鍵暗号化手段にて暗号化処理E1を行い、また、コンテンツCOを、コンテンツ鍵CKを用いてコンテンツ暗号化手段にて暗号化処理E2を行う。すなわち、暗号化コンテンツ鍵ECK i =E1(MK i 、CK) ($i=1, 2, \dots, n$) 暗号化コンテンツ ECKO=E2(CK、CO)である。ここで、 m を、鍵 k で暗号化処理Eで暗号化した結果が c であるとき、 $c=E(k, m)$ と記す。そして、暗号化したコンテンツECKOと、暗号化した n 個のコンテンツ鍵ECK1、…、ECK n を含むデータであるカプセルデータをコンテンツ蓄積部に出力する。

【0023】送信部1510は、制御部1520からの送信指示を受けて、インターネットに接続された通信回線1001に、コンテンツ蓄積部1540に格納されたカプセルデータを送信する。

【0024】ユーザ側PC1100における受信部11

10と制御部1120と、コンテンツ処理部1130とは、パーソナルコンピュータ1100のメモリに格納された音楽コンテンツ再生用プログラムが、CPUにより実行されることにより実現される機能であり、コンテンツ蓄積部1550は、パーソナルコンピュータ1500のメモリ又はハードディスクの一領域である。

【0025】音楽コンテンツ再生用プログラムは、受信すべき音楽コンテンツをユーザに選択させたり、選択された音楽コンテンツを再生するか、記録するか等のユーザの指示を受け付けるためのものであり、制御部1120は、キーボードによる提供者の操作を受け付け、これに応じて、音楽コンテンツの受信指示、再生指示、記録指示等を行うものである。

【0026】受信部1110は、制御部1120からの受信指示を受けて、インターネットに接続された通信回線1001からカプセルデータを受信して、コンテンツ格納部1130に格納し、格納場所を制御部1120に通知する。

【0027】コンテンツ処理部1140は、制御部1120から、再生もしくは記録指示とカプセルデータの格納場所についての情報とを受け取ると、まず、第jのマスタ鍵を用いて、暗号化されたn個のコンテンツ鍵ECKi (i=1, 2, …, n) の中の第jの暗号化したコンテンツ鍵ECKjを、鍵復号手段にて復号処理D1を用いて復号し、復号したコンテンツ鍵CKを用いて、暗号化されたコンテンツECOをコンテンツ復号手段にて復号処理D2を用いて復号する。

【0028】すなわち、

$CK = D1(MKj, ECKj)$

$CO = D2(CK, ECO)$

である。ここで、cを、鍵kで復号処理Dで復号した結果がmであるとき、 $m = D(k, c)$ と記す。

【0029】復号したコンテンツを、再生指示の場合スピーカに出力し、記録指示の場合、メモ리카ードライタに出力し、図示していないが、メディアカードライタは、コンテンツを暗号化した上で、メディアカードへ記録する。

【0030】＜データ構造と関連処理＞提供者側PC1500に入力されるコンテンツは、音楽データ、歌詞などのテキストデータ、ビデオクリップなど画像データより構成される。

【0031】図3は、暗号化コンテンツECO生成過程を示すデータフロー図である。同図に示すように、暗号化コンテンツECOは、平文であるコンテンツCOを、コンテンツ鍵CKで暗号化することにより生成されるデータである。CKは56ビットの鍵データであり、暗号化はブロック暗号方式で行い、例えばDES(Data Encryption Standard) アルゴリズムが用いられる。

【0032】なお暗号化の際、コンテンツは、64ビット

ト毎のデータブロックに分割され、分割されたデータブロックがそれぞれ、56ビットのコンテンツ鍵CKを用いて暗号化され、64ビットの暗号化されたデータブロックが生成される。こうして得られる64ビットの暗号化された各データブロックは結合され、暗号化コンテンツとして出力される。

【0033】また56ビットのコンテンツ鍵CKは、コンテンツ処理部において、例えば各コンテンツ毎に固有に生成される。

【0034】図4は、暗号化コンテンツ鍵ECKiの生成過程を示すデータフロー図である。同図に示すように、暗号化コンテンツ鍵ECKiは、コンテンツ鍵CKを、マスタ鍵MKiで暗号化することにより生成されるデータである。MKiは、例えば112ビットの鍵データであり、暗号化は公開鍵暗号方式の1種である楕円曲線暗号アルゴリズムが用いられる。このとき、提供者側PCのコンテンツ処理部では、マスタ鍵MKiとして、楕円秘密鍵もしくは楕円公開鍵のうちのどちらかを用い、利用者側PCのコンテンツ処理部では、マスタ鍵MKiとして、対応する楕円公開鍵、もしくは対応する楕円秘密鍵のうちのどちらか一方を用いる。

【0035】なお、楕円暗号については、Douglas R. Stinson著「暗号理論の基礎」(共立出版株式会社)に詳細に説明されている。

【0036】なお、同図では示していないが、コンテンツ鍵に管理情報を含めて同様に暗号化してもよい。

【0037】ここで、管理情報は、コンテンツに関連した情報であり、コンテンツの復号条件情報、課金情報を含む。復号条件情報は、コンテンツを復号する条件を示す情報であり、復号することを許容する期日、回数などを示す情報である。また課金情報は、コンテンツを復号する際に請求されるべき料金に関する情報、即ち、音楽コンテンツの使用料金や購入料金を示す情報である。

【0038】＜鍵更新時の処理＞ユーザ側PCのマスタ鍵MKjが、何らかの理由で暴露され更新する必要がある場合に対応するため、ユーザ側PCのコンテンツ処理部1530は、制御部1520から、鍵更新指示と、無効にすべきマスタ鍵MKj、および、オプションとして新しいマスタ鍵MKN+1を受け取ると、鍵暗号化手段において用いるマスタ鍵MK1、MK2、…、MKNのうち、MKjの使用を中止するとともに、オプションとして新しいマスタ鍵MKN+1を受け取った場合は、鍵暗号化手段においてMKN+1をあたりに使用するようにすることもできるものである。

【0039】また、提供者側PCのコンテンツ処理部1130は、制御部1120から、鍵更新指示と、無効にすべきマスタ鍵MKj、および、オプションとして新しいマスタ鍵MKN+1を受け取ると、鍵暗号化手段において用いるMKjの使用を中止するとともに、オプションとして新しいマスタ鍵MKN+1を受け取った場合

は、鍵暗号化手段においてMK $n+1$ をあたりに使用するようにする。

【0040】以上の構成により、鍵更新された提供者側PCで生成されるカプセルデータは、鍵更新されたユーザ側PCを用いてしか、再生記録できないようにすることができ、これによりユーザPC側のマスタ鍵の暴露への対処が可能となる。

【0041】また、図5に、コンテンツ更新装置の構成を示す。

【0042】同図に示すようにコンテンツ更新装置1600は、CPU、メモリ、ハードディスク等を内蔵し、コンテンツ提供者の指示に応じて音楽コンテンツ更新プログラムを実行することができるものであり、提供者側PC1500と接続されている。あるいは、提供者側PC1500そのものであってもよい。

【0043】コンテンツ更新装置は、制御部1610と、コンテンツ処理部1620とから構成される。制御部から、コンテンツ更新指示と、カプセルデータと、無効にすべきマスタ鍵MK j を受け取ると、カプセルデータにおける暗号化コンテンツ鍵CK j を無効にするものである。

【0044】以上の構成により、鍵更新前に提供者側PCで生成されるカプセルデータについても、鍵更新されたユーザ側PCを用いてしか、再生記録できないようにすることができ、これによりユーザPC側のマスタ鍵の暴露への対処が可能となる。

【0045】以上、本発明に係わる著作物保護システムについて、実施の形態である音楽コンテンツ配信システムに基づいて説明したが、本発明はこれらの実施の形態にかぎられないことは勿論である。即ち、

(1) 本実施の形態では、送信部1510、制御部1520、コンテンツ処理部1530、コンテンツ蓄積部1540は、パーソナルコンピュータ1500により実現されるものとしたが、パーソナルコンピュータ1500は、メモリ及びCPUを備えプログラム実行制御機能を有する機器であればよく、また、受信部1110、制御部1120、コンテンツ処理部1140、コンテンツ格納部1130、はパーソナルコンピュータ1100により実現されるものとしたが、パーソナルコンピュータ1100は、メモリ及びCPUを備えプログラム実行制御機能を有する家電機器であればよく、例えば、インターネット接続機能をもつテレビ受信機であってもよい。

【0046】また、本実施の形態における、メモリカードに音楽データを記録するメモリカードライタは、PCカードであるとしたが、これに限定されることはなく、パーソナルコンピュータと接続可能な機器であればよく、例えばUSB(Universal Serial Bus)等により接続される機器であればよい。

【0047】(2) 本実施の形態では、コンテンツ鍵が56ビット、マスタ鍵が112ビット等と、鍵データに

ついて長さを示したが、この長さに限定されることはない。また本実施例における暗号アルゴリズムもDESや楕円曲線暗号に限定されることはない。

【0048】(3) 本実施の形態では、カプセルデータは、通信回線を通じて送られるものとしたが、これに限定されることはなく、例えば、光ディスクなどの記録媒体に格納されるものであってもよい。この場合、送信部1510は、カプセルデータを記録媒体に記録するようにし、受信部1110は、カプセルを記録媒体から読み出しコンテンツ格納部に格納するようなものであればよい。

【0049】(4) 本実施の形態では、メモリカードライタを用いてメモリカードに記録するものとしたが、これに限定されることはなく、例えば、光ディスク記録ドライブを用いて光ディスク等の記録媒体に記録するものとしてもよい。

【0050】(5) 本実施の形態では、コンテンツを暗号化するものとしたが、コンテンツの一部を暗号化するものとしてもよい。

【0051】(6) 本実施の形態では、提供者側PCにおいてあらかじめ複数のマスタ鍵を保持している構成としたが、これに限定されることはなく、単数であってもよい。

【0052】また、提供者側PC装置におけるコンテンツ生成プログラム、及び、ユーザ側PC装置におけるコンテンツ再生プログラムは及びパーソナルコンピュータを介して外部ネットワークからダウンロードできるようにしてもよく、マスタ鍵の更新されたプログラムをダウンロードして利用することにより、マスタ鍵の更新を実現してもよい。また特定のマスタ鍵を削除する機能を有するものであってもよい。またマスタ鍵を取り込む際、署名情報を確認し、正当な場合のみマスタ鍵を取り込むこととしてもよい。

【0053】また、提供者側PC装置におけるコンテンツ生成プログラム、及び、ユーザ側PC装置におけるコンテンツ再生プログラムを実行するためのマスタ鍵などのデータ、もしくは、プログラムを、各PC装置に着脱可能なハードウェアにおいて実行するようにしてもよく、鍵の更新されたハードウェアをPCに装着することにより、鍵更新を実現してもよい。

【0054】

【発明の効果】以上の説明から明らかなように、本発明に係わる著作物保護システムは、デジタル著作物であるコンテンツの配信システムにおける著作物保護システムであって、第1から第 n のマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第1から第 n の暗号化コンテンツ鍵を作成する鍵暗号化手段と、前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、前記第1から第 n のマスタ鍵のうちのいずれかである第 j のマスタ鍵を用いて、前記第 j の暗号化コンテンツ鍵を復号す

ることによりコンテンツ鍵を取得する鍵復号手段と、前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、前記鍵暗号化手段および前記鍵復号手段で利用される前記第 j のマスタ鍵を無効にするもしくは前記第 j のマスタ鍵を第 $n+1$ のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする。

【0055】これにより、鍵更新された提供者側PCで生成されるカプセルデータは、鍵更新されたユーザ側PCを用いてしか、再生記録できないようにすることができ、これによりユーザPC側のマスタ鍵の暴露への対処が可能となる。

【0056】また、著作物保護システムはさらに、前記鍵暗号化手段で作成された第1から第 n の暗号化コンテンツ鍵のうち前記第 j の暗号化コンテンツ鍵を無効にする、もしくは、前記第 j の暗号化コンテンツ鍵を、コンテンツ鍵を第 $n+1$ のマスタ鍵を用いて暗号化した結果である第 $n+1$ の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることとすることもできる。

【0057】これにより、鍵更新前に提供者側PCで生成されるカプセルデータについても、鍵更新されたユーザ側PCを用いてしか、再生記録できないようにすることができ、これによりユーザPC側のマスタ鍵の暴露への対処が可能となる。

【0058】また、前記鍵暗号化手段もしくは前記鍵復号手段は、それぞれ鍵暗号化用もしくは鍵復号用のソフトウェアを実行するパーソナルコンピュータで構成さ *

*れ、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化用もしくは鍵復号用のソフトウェアが、前記第 $n+1$ のマスタ鍵を利用した前記鍵暗号化用もしくは鍵復号用のソフトウェアに置き換えられることとすることもできる。

【0059】これにより、ソフトウェアのダウンロードにより、盗難などで暴露された鍵を無効にするとともに、新しい鍵に更新することが可能となる。

【0060】また前記鍵暗号化手段もしくは前記鍵復号手段は、それぞれ鍵暗号化もしくは鍵復号処理を実行するハードウェアで構成され、前記鍵制御手段により、前記第 j のマスタ鍵を利用した前記鍵暗号化もしくは鍵復号処理が、前記第 $n+1$ のマスタ鍵を利用した前記鍵暗号化もしくは鍵復号処理に切り替えられることとすることもできる。

【0061】これにより、ハードウェアの交換により、盗難などで暴露された鍵を無効にするとともに、新しい鍵に更新することが可能となる。

【図面の簡単な説明】

【図1】本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システムの概観図

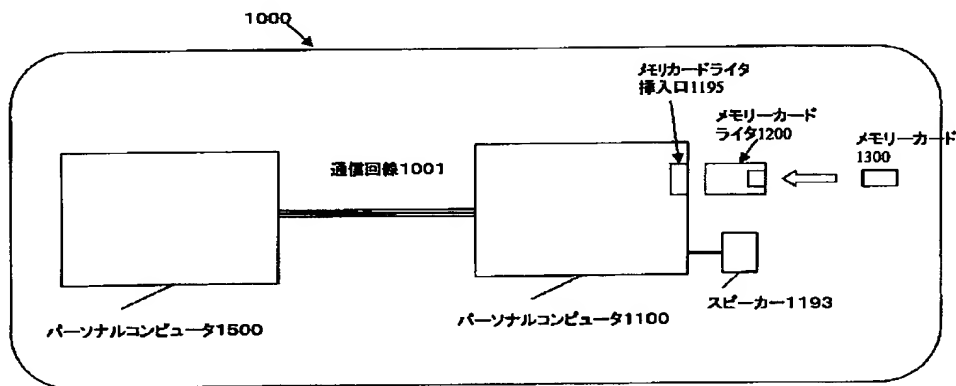
【図2】音楽コンテンツ配信システムの機能ブロック図

【図3】暗号化コンテンツ、及び、暗号化コンテンツ鍵の生成過程を示すデータフロー図

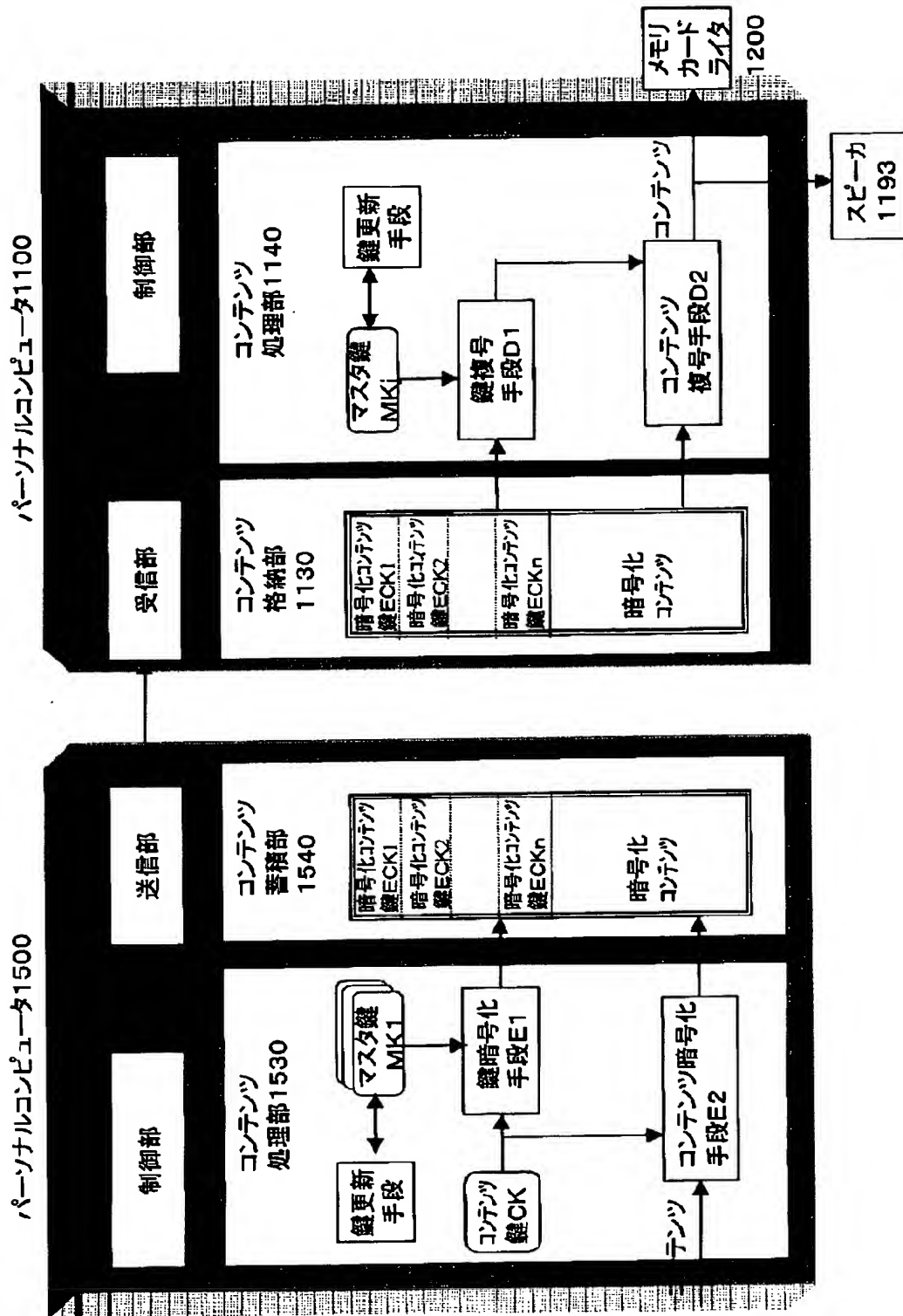
【図4】暗号化コンテンツ鍵ECKiの生成過程を示すデータフロー図

【図5】コンテンツ更新装置の機能ブロック図

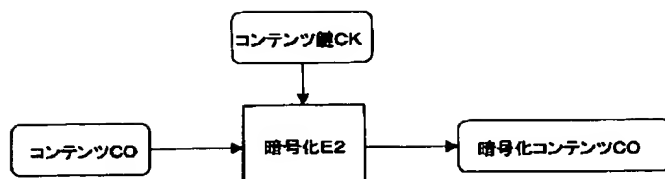
【図1】



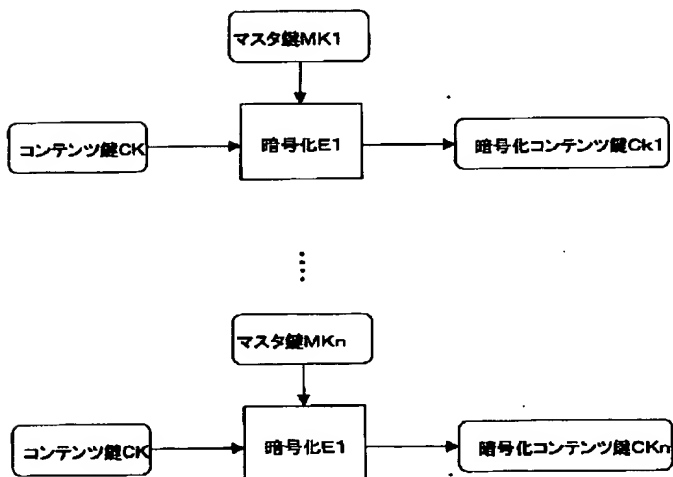
【図2】



【図 3】



【図 4】



【図5】

パーソナルコンピュータ1600

